Case Report

National Gallery DC

### Tracy’s iPhone [2012-07-15-National-Gallery]

# Table of Contents

[Case Report](https://docs.google.com/document/d/1H528_nPqhfp_eOCzvyviwx5U3M1NiPTGtIFaoQoANbY/edit#heading=h.8mjg1w2w81ai)

[National Gallery DC](#_lrib8gqk2z7b)

[Tracy’s iPhone [2012-07-15-National-Gallery]](#_219o4hryceis)

[Table of Contents](#_786gzvga2e8h)

[Executive Summary](#_ccs3x82xm1tu)

[Equipment and Tools](#_hw4rzs3hh4tn)

[Details of Tracy’s iPhone](#_ebsdggfieq5h)

[Evidence to Establish Personas](#_qixiazcd0tiw)

[Evidence relating to theft of valuable stamps](#_5ri2s3hfb3bw)

[Evidence relating to defacement of museum art](#_kt32233q8aao)

[Plot Timeline](#_nz1crxu2ypd4)

[Conclusion](#_m5r3zcqmj9ou)

Appendix A: [Correspondence Evidence](#_w4pkinqwxqi8)

Appendix B: [WiFi and GPS Location Information](#_f8fx30pgaw29)

# Executive Summary

On January 21, 2016, Digitech Inc. was called in to assist the National Gallery, Washington D.C. (NGDC) case involving the conspiracy associated with the theft of valuable stamps and defacing of museums are at the NGDC.

* Tracy is a suspect in the aforementioned conspiracy.
* As part of the investigation, Tracy’s iPhone was taken into custody.
* Digitech, Inc. was tasked with investigating evidence relevant to the aforementioned conspiracy.

As described fully in the report, Digitech, Inc. made the following findings.

[Provide a brief summary of your findings here.]

**Performed a Digital Forensics analysis of Tracy’s phone. Inside was evidence of conspiracy to commit insurance fraud with several other accomplices assisting in the crime.**

### Equipment and Tools

<Briefly summarize the equipment and tools you used to gather and analyze the evidence.>

**Programs and tools used were Kali linux, Autopsy Digital Forensics, and Sqlite Browser. Files that were needed for providing evidence were extracted from Autopsy and then were displayed on the Sqlite Browser for further evidence gathering.**

# Details of Tracy’s iPhone

[Add Tracy’s iPhone Details worksheet from Day 2 here.]

# Case Name: 2012-07-15-National-Gallery Case #: 1EZ215-P

## Details of Tracy’s iPhone

|  |  |  |
| --- | --- | --- |
| **Name** | **Findings** | **Location in iPhone image file** |
| Model | iPhone (1-2) | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/Logs/AppleSupport/general.log |
| Host Name | Tracy Sumtwelves iphone | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/Logs/AppleSupport/general.log |
| OS Version | iPhone OS 4.2.1 (8C148) | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/Logs/AppleSupport/general.log |
| Install Time | 6/6/2012 19:03:28 | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/Logs/AppleSupport/general.log |
| User Email | [tracysumtwelve@gmail.com](mailto:tracysumtwelve@gmail.com)  tracysumtwelve@nationalgallergydc.org | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/Mail |
| Phone Number | +1 (703) 340-9661 | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/Logs/AppleSupport/general.log |
| Serial Number | 86004482Y7H | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/Logs/AppleSupport/general.log |
| ICCID | 89014103255195342366 | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/logs/lockdownd.log.1 |
| IMEI | 01202 | /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/root/Library/Lockdown/activation\_records/wildcard\_record.plist |
| MD5 Hash | 34c4888f095dc3241330462923f6fea5 | History.plist, under the FILE METADATA |
| SHA256 Hash | 71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607 | History.plist, under the FILE METADATA |

# Evidence to Establish Personas

This section establishes aliases, phone numbers, emails addresses associated with each person, and relationships between each individual.

Tracy:

Phone Number: (703) 340-9961

Personal Email: tracysumtwelve@gmail.com

Work Email: tracy.sumtwelve@nationalgallerydc.org

Relationship: Accused, Alias is Coral

Pat:

Phone Number: **(571) 308-3236**

Email: [**patsumtwelve@gmail.com**](mailto:patsumtwelve@gmail.com)**, Alias email perrypatsum@yahoo.com**

Relationship: **accomplice, in the SMS.db pat references tracy as sis (Brother to the Accused)**

Terry:

Phone Number: **(703)829-6071**

Email: **N/A**

Relationship: **accomplice, tracy’s daughter**

Joe:

Phone Number: **N/A**

Email: **joe.sum.twelve@gmail.com**

Relationship: **accomplice, tracys Ex Husband**

Carry:

Phone Number: **(202) 275-2124**

Email: **carrysum2012@yahoo.com**

Relationship: **accomplice, coworker in the museum**

**King:**

**Phone number: N/A**

**Email:** [**Throne1966@hotmail.com**](mailto:Throne1966@hotmail.com)

**Relationship: acquaintance of Pat, met in Jail, being blackmailed**

[Provide a summary of your conclusions here.]

**The accused individuals attempted to commit $289k worth of stamp insurance theft fraud**

# Evidence relating to theft of valuable stamps

This sub-section provides details regarding the evidence found as it relates to the theft of valuable stamps.

[Provide a summary of your conclusions here. Refer to specific artifact numbers from Appendix A and B (see below) to support your conclusions.]

**Path: /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Media/DCIM/100APLE , right click on image and open with External Viewer and there are pictures of the stamps that were going to be stolen**

**Path:/img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@**[**pop3.live.com/INBOX.mbox/Attachments/61/3/docs.zip/docs**](http://pop3.live.com/INBOX.mbox/Attachments/61/3/docs.zip/docs) **, contains 3 Stamp Insurance PDF email file attachments**

# Evidence relating to defacement of museum art

This sub-section provides details regarding the evidence found as it relates to the defacement of museum art.

[Provide a summary of your conclusions here. Refer to specific artifact numbers from Appendix A and B (see below) to support your conclusions.]

**Path: /img\_tracy-phone-2012-07-15-final.E01/vol\_vol5/mobile/Library/Mail/IMAP-tracysumtwelve@gmail.com@**[**irnap.gmail.com/INBOX.irnap.gmail.com/Messages**](http://irnap.gmail.com/INBOX.irnap.gmail.com/Messages)

**PLEASE REFER TO IPHONE EVIDENCE FOLDER FOR PICTURES OF STAMPS TO BE DEFACED**

# Plot Timeline

[Provide an outline of the key events in the order they occurred. Note the date of each event.]

**PLEASE REFERENCE WORKSHEET DATES AND TIMELINES FOR ORDER OF EVENTS**

# Conclusion

Evidence found on Tracy’s iPhone indicated the following:

* [Summarize your final conclusions of the case and Tracy’s Iphone here.]
* [For example: Tracy used the alias Coral and Pat used the alias Perry.]

**Tracy used family members to steal expensive stamp collection and collect insurance money to pay for Terry’s(her daughters’) expensive school (Prufrock) tuition.**

**Carry bribed Tracy to sneak in a tablet to record and post online a flash mob at the art gallery in hopes to deface and embarrass the Gallery**

# Appendix A: Correspondence Evidence

This subsection will provide an amalgamation of the email and SMS corresponce evidence.

[Paste your Correspondence Evidence Worksheet here.]

**Please reference EMAILS TIMELINE WORKSHEET**

# Appendix B: WiFi and GPS Location Information

[Paste your GPS Evidence Worksheet here.]

**Please reference LOCATION INFORMATION WORKSHEET for phones WIFI and GPS info**